

**ATINER's Conference Paper Proceedings Series**

MED2017-0019

Athens, 22 August 2017

**The Control of Expression in New Media Era:  
A Research Based on Real-Name System in China**

Lei Lili and Zheng Baozhang

Athens Institute for Education and Research  
8 Valaoritou Street, Kolonaki, 10683 Athens, Greece

ATINER's conference paper proceedings series are circulated to promote dialogue among academic scholars. All papers of this series have been blind reviewed and accepted for presentation at one of ATINER's annual conferences according to its acceptance policies (<http://www.atiner.gr/acceptance>).

© All rights reserved by authors.

**ATINER's Conference Paper Proceedings Series**

MED2017-0019

Athens, 22 August 2017

ISSN: 2529-167X

Lei Lili, Lecturer, Dalian University of Technology, China  
Zheng Baozhang, Professor, Dalian University of Technology, China

**The Control of Expression in New Media Era:  
A Research Based on Real-Name System in China**

**ABSTRACT**

In China, newspapers, televisions are all in the charge of the State Administration of Press, Publication, Radio, Film, and Television of The People's Republic of China. There is almost no obstacle for the government to make the public opinion under control. This control can be achieved by licensing system, appointing editors as gatekeeper, or by administrative order. But the development of internet greatly challenged the previous approach of this control. Chinese authority searches for new way to deal with the online voices. The process of the establishment of real name-registration system in China reveals the approach that the authority tried to control public opinion, and to keep the dissidents under surveillance. "Ordinance of Micro-blog Development Management in Beijing" was issued and implemented on December 16, 2011. According to this ordinance, real identity information should be offered when registering micro-blog account; otherwise, no information should be produced, reproduced, published, or disseminated. This is called Real-Name System, and it aroused heated debates. One year later, the Standing Committee of the National People's Congress promulgated and implemented "Decision on strengthening the network information protection". On November 7th, "Cybersecurity Law", according to which network operators need to ask users to provide identity information, and the government will issue effective strategy to promote the mutual recognition between different electronic authentications. Thus, Real-Name System is finally implemented by law in China. As Václav Havel said, in the system of post-totalitarianism, power is concealed under the cloak of legal terms. In new media era in China, political control over online speech is achieved in the name of protection for social order and personal safety.

Keywords: Real-Name System, Legislation, post-totalitarianism, cybersecurity, freedom of expression

## **Introduction**

Real name-registration became a public topic since 2002. An article published by Li Xiguang, professor from Tsinghua University, said that the internet should use real name-registration system, anonymous expression on the internet should be forbidden. (Li Xiguang: 2002). This argument evokes controversy, but it did not last too long. Li Xiguang changed his mind and said it is infeasible to prohibit anonymous expression online because of legal and technical barriers.

In 2009, Micro-blog (which is called Chinese twitter) was introduced into China, and very quickly, it became a significant approach of disseminating and receiving information, even some significant news were first disseminated on Micro-blog, such as Wenyong D-train accident on July 23<sup>rd</sup> 2011. Some users even take Micro-blog as a portal to get information. What came along with this phenomenon is the optimistic expectation that Micro-blog may generate democracy in China.

On December 16th, 2011, “Ordinance of Micro-blog Development Management in Beijing” was issued and implemented. According to this ordinance, net users should offer their real identity information when registering micro-blog account; otherwise, no information should be produced, reproduced, published, or disseminated. This is called “Real-Name System”, and it aroused heated debates. One year later, the Standing Committee of the National People's Congress promulgated and implemented “Decision on strengthening the network information protection”. Accordingly, real-name system is fixed by law in China. As Václav Havel said, in the system of post-totalitarianism, power is concealed under the cloak of legal terms. In new media era in China, political control over online speech is achieved in the name of protection for social order and personal information. On November 7<sup>th</sup> 2016, “Cyber Security Law” was issued and it will come into effect on 1<sup>st</sup> June 2017. According to Cyber Security Law, network operators need to ask net users to provide identity information, and the government will issue effective strategy to promote the mutual recognition between different electronic authentications. Thus, network-operators become a co-regulator of cyber space. This paper examines Real-Name System as a growing field of internet legal practice. By analyzing and querying the generating process of real-name system, deduce the effect it will bring to the development of internet and to the freedom of expression.

### **“Ordinance of Micro-blog Development Management in Beijing”: Initial Attempts to Real-name System**

On December 16<sup>th</sup> 2011, “Ordinance of Micro-blog Development Management in Beijing” was issued by Pekin News Office, Police Security Bureau, the Administrative Bureau of communication and the Information Office of Internet. It came into effect on the same day. The 9<sup>th</sup> article of this

ordinance states, “Every organization or everyone shall register in his/her/its real identical information (in China this means real ID number), registration in false or faked identical information are not permitted, when he/she/it produces, duplicates, disseminates, or broadcasts information on the internet.” This is called “Micro-blog real-name system”, and it evoked social discussion.

However, as this regulation was implemented, “Micro-blog real-name system” came into effect, the optimistic expectation that Micro-blog may generate democracy in China faked away. Xiewen, the ex-CEO of Yahoo in China said, to treat Micro-blog as traditional media can throttle the vigor of new media, and what is more, it may prevent the process of informatization in China (Xiewen: 2011).

At the beginning this ordinance, it states, “This ordinance is drawn up according to ‘Telecommunication regulations’, ‘Measures for the administration of Internet information service’ and other laws, acts, rules, regulations, and the actual situation of Pekin.” “Telecommunications regulations” and “Measures for the administration of Internet information service” are administrative rules and regulations issued in 2000. But Micro-blog came into being in 2009, 9 years after those two regulations. In the reply to the question about what is the legal foundation of the regulation, the authority issued the ordinance said, article 59 (4) of “Telecommunication regulations” states, No one or organization can take actions as follows, ... (4) access to the internet service and use mobile phone by registration in false or fake ID. In accordance with this article, the user of Micro-blog should disseminate information after registration in real identical information. Obviously, this is a severe misrepresent of article 59 (4) of “Telecommunication regulations”. Because “Telecommunication regulations” only requires people register in real ID when access to internet, but the authority broadened the scope of “real-name system” to disseminating information in Micro-blog. The other regulation stated as the foundation of this ordinance is “Measures for the administration of Internet information service”. It was promulgated to regulate the internet service provider, never touched upon the user’s rights or obligations in using the internet. This means the implementation of this ordinance was not empowered by superior legislations.

Besides, the first article of the ordinance states that the original intention of the ordinance is to regulate the online service of Micro-blog, to preserve the online communication order, to safeguard online information, to protect the service providers and Micro-blog users, to meet the public demands for online information, to promote the benign development of the internet. The authority said, with the development of Micro-blog, some problems that harmed the public interests emerged, such as dissemination of rumors or false information, transaction of “fans”, online cheating. Websites, users and the public are resentful about these phenomena; they call for supervision of online service, to safeguard the development of the internet. That’s why this ordinance was issued.

Actually, the dissemination of rumors or false information has being exist since human came into being, long before Micro-blog appeared. Apparently,

there is no causal relationship between Micro-blog and these negative phenomena. In traditional acquaintance society, when people communicate with each other in their real identities, or even face to face, rumors are prevalent sometimes, so anonymous communication is not the true reason of rumors, and to prevent rumors or false information by “real name system” is something like treating the foot when the head aches.

Besides, chilling Effect is an unavoidable consequence come along with “Real-name system” that may be harmful to the society. Even if it can prevent rumors to some limited extent, it may leave more shady deal concealed. In the background of China today, where corruption is so severe and power is not under effective supervision by the public, it is more urgent to make sunshine law to make the government transparent, rather than to establish “real-name system” to prevent rumors, not to mention that it is not an available approach to deal with online rumors.

In the technological background of web2.0, Micro-blog has generated “self-rectification mechanism” that most false information can be rectified very soon in the consequent information after it was released. In recent years, there were several online rumors, such as taking salt with iodide can prevent nuclear radiation, Aids patients from Xinjiang province put their blood in food, and Lang Xianping, an economist accepted 2,000,000 from Guo Meimei, a girl showed off her fortune online and was suspected involving in corruption and arrested afterwards because of holding gambling house. But these rumors were all rectified very soon and caused almost no damage. Even if there were negative consequences, they can be remedied by judicial action.

Another consequence comes along with real-name system is the risks it brings to the safety of private information of net users. China should take warning from the experiences of South Korea. In 2007, in order to make people be responsible for their online expression, regulations were made in Korea which demand people who use the websites and online forum that have more than 100,000 users register in real name. After this “real-name system” was implemented, a lot of private information was divulged. August 11<sup>th</sup> 2011, 35,000,000 users’ private information was leaked, including users’ name, telephone number, e-mail code and ID number. Besides, this real-name system was judged unconstitutional by the constitutional court in 2010. Therefore, in 2011, 4 years after the “real-name system” was promulgated, it was abolished.

According to the Xinhua news agency, on December 25<sup>th</sup> 2011, unprecedented great leakage of users’ data appeared in China, more than 50,000,000 accounts and passwords of internet users were disclosed<sup>1</sup>, and from January to June in 2011, there were more than 121,000,000 accounts or passwords of internet users were stolen.<sup>2</sup>

Shi Xiaohong, vice-president of Qihu 360 Company, a corporation concentrates on the safeguard of the internet, said that besides these 50,000,000 accounts, there were still numerous users’ information were stolen but not

---

<sup>1</sup> [http://news.xinhuanet.com/legal/2011-12/25/c\\_111297899.htm](http://news.xinhuanet.com/legal/2011-12/25/c_111297899.htm)

<sup>2</sup> [http://news.xinhuanet.com/legal/2011-12/25/c\\_111297899\\_2.htm](http://news.xinhuanet.com/legal/2011-12/25/c_111297899_2.htm)

dispatched. Surveys held by Qihu 360 Company shows that about 60-70% of the Chinese websites have security loopholes, their safety precautions are not sufficient enough. In the storage of users' information, some big websites use encipherment storage technology, even when the information was stolen, it can not be settled.

According to introduction of Qihu 360 Company, stealing of websites' database is a very common way to attack the websites in recent years; it is more dangerous than Trojan horse virus. Among the internet users whose accounts were stolen, more than 80% due to the cleanout of the whole database by hackers<sup>3</sup>. So, it is careless for the ordinance to issue this "real-name system" without considering the consequences may come along with it.

According to rules for legislative process of regulations issued in 2002, in order to collect the views of relevant agencies, organizations or citizens, hearing should be held before drafting regulations. If the regulations being drafting are related directly to the vital interests of citizens, legal persons or other organizations, relevant agencies, and they hold different views on the issues involved in the regulations, the draft should be made public for consultation. Besides, regulations should come into effect 30 days after it is released, unless it involves the national security, foreign exchange rates, monetary policy, or it will impede the implement of the regulations if it does not come into effect immediately. Since there had being fierce controversy about the online real-name system since 2002, and it has no relationship with the national security, foreign exchange rates, monetary policy, therefore, according to the principles mentioned above, the ordinance should be made public to seek for opinions, and it should be implemented 30 days after it was promulgated. But the fact is it came into effect immediately when it was released.

What's more, according to the legislative law, the authorities issued the ordinance has no power to draw up such regulations, and they are not authorized by higher law in making such laws. As an important human right, the freedom of expression is protected by the constitution, the Pekin authorities obviously acted beyond their powers.

### **Draft Amendment of "Regulation on Internet Information Service": Purpose and Intended Effect**

On June 7<sup>th</sup>, 2012, the National Internet Information Office and the Ministry of Industry and Information Technology issued a notice on the Draft Amendment of "Regulation on Internet Information Service" (hereinafter referred to as the "revised draft") to solicit opinions. The "revised draft" is the first revision of the original "Regulations on Internet Information Service" implemented on Sept. 25<sup>th</sup>, 2000 (hereinafter referred to as "original regulation").

---

<sup>3</sup> [http://news.xinhuanet.com/legal/2011-12/25/c\\_111297899\\_2.htm](http://news.xinhuanet.com/legal/2011-12/25/c_111297899_2.htm)

In contrast to "original regulation", the "revised draft" has changed in several aspects. First, this reflected in their first articles which declare the purposes of their legislation are different. "Original regulation" illustrated that the purpose of the regulation is "to regulate the internet information services activities to promote the healthy and orderly development of internet information services", while "revised draft" provides that it is "in order to promote the healthy and orderly development of internet information services, safeguard national security and public interest, protect the legitimate rights and interests of the public and internet information service providers, regulate the internet information service activities." Obviously, the purpose of "revised draft" is enlarged. So it can be deduced that the "revised draft" aims to better serve these two new purposes. Then how does the "revised draft" serve these two legislative purposes?

Article 10 (1) of the "revised draft" stipulates that who provide internet news information services, provide services that internet users can dispatch information to the public("provide services that internet users can dispatch information to the public" including but not limited to forums, blogs, micro-blog), and provide search services of internet information need permission approval from internet information content department. Article 15 of the "revised draft" stipulates that "Internet information service providers who provide information services by internet users to the public should require users to register with real identity information". This means net users need to registration with the authentic ID information. According to this article, users should register with real identity information when they use of forums, blogs, Micro-blog and other interactive services.

For the internet service providers, this mandatory requirement for real-name registration is actually an intervention in the autonomy of the right to operation of their company. Whether the Internet service provider requires the user to provide real identity information or not is the right of network operators. So, it is unreasonable intervention of right of enterprise management. Moreover, even though the "revised draft" is just set obligations for net operators, and it does not demand net users to do anything, but all net users who use the internet need to fulfill the additional obligations, which is undoubtedly constitutes interference of people's right to speech, and freedom of expression, which set up conditions for freedom of the press online.

According to the explanation of the law-maker, since Dec. the year before, Beijing, Shanghai, Tianjin, Guangzhou, Shenzhen and other five cities pilot implementation of the micro-blog users with real-name system, and it shows that real-name system is effective in beating online criminal activities, purifying the network environment, strengthening the sense of responsibility of users, and promoting the integrity of social construction, it played a positive role.

Article 16 of the "revised draft" adjusted the duration of the record retention that net operators need to keep, "internet information service providers should record the information and services issued by itself and its service objects, and save them for 6 months", "the internet access service

provider should record the log information, and save them for 12 months, and provide technical support for the public security organs, the state security organs to search in accordance with the law". It can be inferred from this regulation that the purpose of the amendment is actually for the convenience of law enforcement, and it set an additional obligation for the internet service providers. Real ID registration is indeed make law enforcement more convenient, but this system ignored a great disadvantage, a large number of net users' information are exposed to net operators, the disclosure put the users in serious risk. It is not responsible towards the safety of citizens' personal information. When net users' personal information is leaked, they can hardly find who leaked it, because people are impossible to use the online services from only one net operator.

Article 17 of the "revised draft" states, "internet information service providers, internet access service providers are obligated to keep the user's identity information, log information and other personal information secret, they should not sell, tamper, deliberately leak or illegally use the user's personal information." According to the maker of the regulation, such regulation is to protect personal information, prevent disclosure and illegal use of personal information. The question is, if net user does not need to register the true identity information, their personal information can be protected better, and they can effectively avoid such security risks. Then why the regulations make such a contradictory arrangement? Based on this, we can deduce that this provision is intended to dispel people's scruple about the real-name registration system. However, the security risks of users' information are not primarily due to the internet information service providers who can not be kept confidential or illegally used. Because we can see from the previous user information leak event, which is mostly caused by hacker attacks, and there is no evidence show the internet service provider should be blamed.

From a technical perspective, if the authority can find the hacker after attack, it can also find people who publish dangerous information online, and even easier, because hackers know better how to conceal themselves than ordinary net users. Therefore, people who publish illegal speech online can be traced without real-name registration which will make the users information in danger. Thus, the actual effect of real-name system is to restrict free speech and to help the public security organs finding scaremongers or other suspects who disseminate illegal information online. Therefore, to demand net operators keep net users' information secret in order to dispel the public's anxiety about their personal information is unreasonable and unconvincible. We can conclude that the "revised draft" is more stringent on the internet's information control, but it does not help or even hamper the claims "Safeguarding national security and public interest, protecting the legitimate rights and interests of the public and Internet information service providers". Therefore, to achieve good governance of the internet, more practical and effective legislations are needed.

**“Decision on strengthening the network information protection”: Real-Name System become applicable nationwide**

On Dec. 28<sup>th</sup> 2012, the Standing Committee of the National People's Congress issued “Decision on strengthening the network information protection”. This decision came into effect immediately. In China, the degree of legal effect of decisions issued by the Standing Committee of the National People’s Congress equals to law. At the beginning of this decision, it states that its purpose is to protect the security of network information, to protect the legitimate rights and interests of citizens, legal persons or other organizations, and to safeguard national security and public interest. The "decision" includes 12 articles. Article 12 stipulates that the “decision” come into effect since the date of implementation; Article 11 provides responsibilities of violating the "decision". The remaining 11 are all substantive provisions of which Article 1 to Article 10 is the rights and obligations. It is noteworthy that, except article 8 and article 9 which provide that citizens encounter violations of personal information can seek relief, can report, accuse, the remaining 8 articles are all set obligations (as shown in the table below).

Article	Subject	Obligation
1	The state	Protect electronic information that identifies citizenship and personal privacy.
	Any organizations or anyone	Shall not steal or obtain personal electronic information by other illegal means, shall not sell or illegally provide personal electronic information to others.
2	ISPs and other enterprises and public institutions	The collection and use of personal electronic information in the business activities shall follow the principle of legitimate, fair and necessary, indicate the purpose, manner and scope of the information collected and used, and they should do this only when they get the consent of the people whose information is being collected, and shall not violate the provisions of laws and regulations and their agreement. Collection and use of personal electronic information should publish the rules about how the information are collected and used.
3	ISPs and other enterprises and public institutions	Citizens' personal electronic information collected in business activities must be kept strictly confidential and shall not be disclosed, tampered, destroyed, sold or illegally provided to others.
4	ISPs and other enterprises and public institutions	Technical measures and other necessary measures should be taken to ensure the security of information and to prevent leakage, damage and loss of personal electronic information collected in business activities. Immediate remedial action should be taken in the possible event of leakage damage or loss of information.
5	ISPs	Strengthen the management of the information issued by

		users; and immediately stop the transmission of the information, take measures such as elimination, and keep the relevant records and report to the relevant authorities in charge when discover the information prohibited by law or regulation.
6	ISPs	If offering access services for fixed telephone, mobile phone and other internet access procedures, or offering dissemination services, require users to provide real identity information when signing agreements or confirming the provision of services with users
7	Any organizations or anyone	Should not send commercial electronic information to fixed telephone, mobile phone or personal e-mail without the consent or request of the electronic information recipient, or if the electronic information receiver expressly rejects it.
10	Relevant departments	Perform their duties in accordance with the law, take technical measures and other necessary measures to prevent, stop and investigate the illegal acts of theft or other illegal means to obtain, sell or illegally provide personal electronic information to others and other illegal or criminal behavior about network information
	ISPs	When the competent authorities perform their duties according to law, the network service providers shall cooperate and provide technical support.
	State organs and their personnel	Keep confidential about the personal electronic information of citizens got by performing-duty behavior; and shall not disclose, tamper, destroy, sell or illegally provide to others.

Most provisions of this decision are obligation norms which set obligations for Internet Service Providers. This is easy to understand. Because ISPs have the most advantages to get in touch with the personal information of citizens, and they incline to make the most benefits from using personal information of citizens due to their profit-driven nature. What is difficult to understand is the 6<sup>th</sup> article. It demands ISPs to ask their users to register the real identity information, when they offering information dissemination service for the users. This means net users need input their ID numbers when they want to express themselves or disseminate information online. Since the purpose of this decision is to protect the security of network information, while the ISPs are the subjects most likely to infringe on the online personal information. Therefore, if the authority wants to protect personal information, it should keep the ISPs away from personal information as much as possible, and make the users less exposed to the ISPs. But what this decision infers is just the opposite. When internet users want to enjoy the service of ISPs to express themselves online, they need to expose them to the ISPs. The real-name system impedes freedom of expression, in the name of protecting personal information. And it does no help to the security of personal information. What's more, this system has a potential hypothesis that all the net users are suspects. It can be included

that, the decision proclaims to protect the personal information, but the solution is to demand users to submit their identification information to ISPs; and ISPs are obliged to keep these information but they can not misuse or leak them out, unless the police or other competent authorities demand it. ISPs are playing a supporting role for the police or other authorities in their official duties.

Now, the conclusion comes out, real-name system is the core part of this decision, and the true intention of the decision is to furnish higher law basis for the “Ordinance of Micro-blog Development Management in Beijing” talked above and Draft Amendment of “Regulation on Internet Information Service”, which is still in amendment. The real-name system reinforced the control to online express, but because it is put forward under the false impression of information protection, so it did not encounter fierce boycott. And because the responsibility of offending the decision is ambiguous, it leaves much room for discretion, it provides the basis for the legitimacy of administrative power to strengthen and expand.

### **Real-name System in “Cyber Security Law”: Is Real-Name System good or bad for Cyber Security?**

With the fast development of ICTs, enormous challenges and risks aroused. In order to serve the problems of network security, China has promulgated and revised several administrative regulations mentioned above to regulate the operation of the network and online communication. However, these legislations were promulgated without sufficient brewing. So they can only take immediate and emergent problems into account, and hardly have any forward-looking considerations. On Nov. 17<sup>th</sup> 2016, the NPC Standing Committee issued Cyber Security Law and it will be implemented on 1<sup>st</sup> Jun 2017. This is the first fundamental law for cyber space in China, so it is called “small constitution” of cyberspace. Its main purpose is to establish cyber security system, promote the construction of network infrastructure, and encourage ICTs innovation and application. Cyber security means electronic data and systems are prevent from attack, loss, or other compromise. Cyber Security Law shows the framework of the legislation of internet in the future. Cyber security is consist of several legal issues, such as privacy concerns, data breaches, and establish a effective strategy for potential cyber security crisis situations and so on. At the beginning, the original intention of real-name system is just to prevent online rumors, but now it is a key pillar to achieve cyber security.

According to Cyber Security Law, there are three subjects in the regulatory relationship, the state, network operators (including network owner, network manager, and internet service provider), and net users. Among them, network operator plays the core role in network regulation. This is very different from the traditional regulatory approach. China’s traditional media like newspaper, magazine, radio and television are mainly regulated by administrative way. But network operators are private enterprises. The administrative regulatory

approach is no longer applicable. Network operator is not administrative authority and they are not public institution. They have no administrative duty and regulatory functions, but in the background of cyberspace, the administrative authorities' regulatory responsibilities are transferred to network operators.

According to Article 23 of Cyber Security Law, the network operators who offer network access service, domain name registration services, and deal with network applications for fixed telephone, mobile phone, or provide users with information dissemination, instant messaging and other services, sign agreements with net users or to confirm the provision of services, should ask net users provide real identity information. If the users do not provide the true identity information, the network operator shall not provide services. According to the "user does not provide real identity information, network operators shall not provide related services" requirements, network operators need to verify the authenticity of user information, but how can they verify? The solution proposed by Cyber Security Law is that "the state will implement a network credible identity strategy that supports research and development of secure, convenient electronic identity authentication technologies that drive mutual recognition among different electronic identities." That means the government will provide support so that the network operator can confirm the authenticity of the user's identity information. Network operators will have the ability to verify whether the net users' registration information is true or false.

With the development of the internet, enterprises engaged in internet services increased rapidly. According to Article 23 of Cyber Security Law, most net operators have plenty of the identity information, but their knowledge about the law, their network security capabilities and internal management level are uneven. This means that a large number of net operators hold much personal information of citizens, but they are unable to protect it effectively, this will undoubtedly bring a huge risk to the net users' personal information security. When a large number of internet companies and practitioners have access to personal information, if the personal information were disclosed, it would be very difficult to trace the disclosure channels of personal information, and it would be difficult to find out who should be blamed. Although the Penal Code incriminates the disclosure of personal information, it can not guarantee the safety of personal network information only by the prohibitive provisions of the law. Therefore, despite the legislation including a large number of prohibitions, but in fact it can not effectively protect the safety of personal information of citizens, because these prohibitive provisions are under the background that massive personal identity information were generally exposed to plenty of net operators. For example, the legislation prohibits the collection of personal information, but to regulate such behavior will undoubtedly require a heavy regulatory cost which the competent authorities can not afford.

### **Concluding Remarks**

In 1993, “New Yorker” published a cartoon which made a brilliant summary about the internet, “On the internet, no one knows you are a dog”. This reflects the key character of the cyberspace then. The biggest difference between real society and cyberspace is the virtuality caused by anonymity. However, in the WEB2.0 age, the situation changed a lot. For the active network users, their expressions and communications in the virtual world have drawn their images. We can not hide ourselves on the internet. So Fang Xingdong, the founder of Blog China said, “In the blog world, everyone knows you are a dog.” Personal information is the channel leading to personal privacy, if someone’s personal information is disclosed sufficiently, he/she has almost no privacy at all.

Of course, personal information and privacy is not unconditional, in some situations, we prefer to give it up to some extent. In order to enjoy other benefits or convenience, people tend to hand over or give up some personal information. For example, we may release our physical privacy in order to treat the disease; we may transfer our identity information to enjoy the convenience that the internet brings. But in these situations, we have the freedom to decide or choose whether we give it up or not. But according to real-name system, we are not allowed to have the right to determine whether we would like to offer our ID to the net operators. Since the net operators are not trustable, if net users register in real identification, they will face serious risks.

Besides, in China, the Internet has long been seen as a social “decompression valve.” Under real-name system, net users may not express their complaints publicly; internet could no longer be the social “decompression valve”. If public opinion can not be vented, the pressure can only flock to the real society; its possible consequences may be more social problems. Although the real-name system is just requiring net users to register with real ID number, but this system reflects the regression of social governance.

In China, newspapers, televisions are all in the charge of the State Administration of Press, Publication, Radio, Film, and Television. There is almost no obstacle for the government to make the public opinion under control. This control can be achieved by licensing system, appointing editors as gatekeeper, or by administrative order. But the development of internet greatly challenged previous approaches of this control. Chinese authority searches for new way to deal with the online voices. The process of the establishment of real-name system in China reveals the approach that the authority tried to control public opinion, and to keep the dissidents under surveillance.